EXHIBIT 3

SYMANTEC'S STATEMENT OF ISSUES OF FACT THAT REMAIN TO BE LITIGATED

Symantec reserves the right to modify, supplement, or change this Statement of Issues of Fact That Remain to be Litigated (the "Statement") to reflect the Court's rulings on any pending dispositive motions. Symantec also reserves the right to modify, supplement or change this Statement to the extent necessary to fairly respond to any new issues SRI raises in its Statement of Issues of Fact. To the extent that any of these issues is deemed an issue of law rather than an issue of fact, Symantec incorporates said issue by reference into Defendants' Statement of Issues of Law that Remain to be Litigated. Conversely, to the extent that any issue in Defendants' Statement of Issues of Law that Remain to be Litigated is deemed an issue of fact, Symantec incorporates said issue by reference into this Statement.

This Statement of Issues of Fact applies only to the liability phase of trial. Issues of damages and willfulness have been bifurcated by the Court and will be addressed separately.

For the Court's convenience, the claims asserted against Symantec will be referred to herein as the "asserted claims." The particular claims asserted against Symantec are:

Claims asserted against Symantec	• '203 patent: claims 1-2, 4, 6, 12-13, 15, 17 • '615 patent: claims 1-2, 4, 13-14, 16

I. INFRINGEMENT

Symantec's iForce IDS, ManHunt 3.0, Symantec Network Security 4.0, and Symantec Network Security 7100 Series appliances will be referred to as the "ManHunt Products."

Symantec's Incident Manager 3.0 and Security Information Manager 9500 Series appliances will be referred to as the "Manager Products."

Symantec's Gateway Security 5400, 5600 and 1600 Series appliances will be referred to as the "SGS Products."

A. ManHunt Products

1. Whether, by a preponderance of the evidence, SRI can prove that Symantec directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by making, using, selling, or offering to sell the ManHunt Products.

2. Whether, by a preponderance of the evidence, SRI can prove that any Symantec customer directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by using the ManHunt Products.

3. Whether, by a preponderance of the evidence, SRI can prove that Symantec, with the requisite intent and knowledge, actively induced its customers to infringe the asserted claims of the '203 or '615 patents by use of the ManHunt products.[1]

B. SGS Products + Manager Products

4. Whether, by a preponderance of the evidence, SRI can prove that Symantec directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by making, using, selling, or offering to sell the Symantec's SGS Products in combination with the Manager Products.

[1] Symantec understands that SRI is no longer asserting contributory infringement against any Symantec product.

5. Whether, by a preponderance of the evidence, SRI can prove that any Symantec customer directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by using the SGS Products in combination with the Manager Products in the manner that SRI alleges to be infringing.

6. Whether, by a preponderance of the evidence, SRI can prove that Symantec, with the requisite intent and knowledge, actively induced its customers to infringe the asserted claims of the '203 or '615 patents by using the SGS Products in combination with the Manager Products.

II. INVALIDITY

7. Whether, for each claim, SRI can prove a date of invention earlier than the respective filing date, and such date of invention.

A. Anticipation

8. Whether the following printed publications and patents are prior art under 35 U.S.C. § 102 (a), (b) or (e):

- P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," ("*Live Traffic*" various versions);
- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20th National Information Systems Security Conference, pp. 353-365, October 9, 1997 ("*Emerald 1997*");[2]
- L. Todd Heberlein et al., "A Network Security Monitor," Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296-304, May 1990 ("*NSM 1990*");
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, pp. 262-271, October 1992 ("*ISM 1992*");
- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol. 8 No. 3, pp. 26-41, June 1994 ("*NID 1994*");
- Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of

[2] The Court previously determined that EMERALD 1997 is a prior art printed publication under 102(b).

Existing Systems and a Proposed Distributed IDS Architecture," CSE-91-7, Feb. 1991 ("*DIDS Feb. 1991*");

- Steven R. Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype," Proc. 14th National Computer Security Conference, pp. 167-173, October 1991 ("*DIDS Oct. 1991*");
- S. Staniford-Chen et al., "GrIDS – A Graph Based Intrusion Detection System for Large Networks," 19th National Information Systems Security Conference, pp. 361-370, October 1996 ("*GrIDS 1996*");
- Steven Cheung et al., "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical Report, UC Davis Department of Computer Science, Davis California, May 14, 1997 ("*GrIDS 1997*");
- "RealSecure Release 1.0 for Windows NT 4.0 A User's Guide and Reference Manual";
- "NetRanger User's Guide Version 1.3.1," WheelGroup Corporation, 1997 ("*NetRanger Manual*").[3]

9. Whether the following systems or products were known or used before the inventions claimed, or were in public use or on sale prior to November 9, 1997:

- Network Security Monitor ("NSM");
- Distributed Intrusion Detection System ("DIDS");
- Graph-based Intrusion Detection System ("GrIDS");
- NetRanger;
- ISS RealSecure;

10. Whether, by clear and convincing evidence,[4] Symantec can prove that the above-listed printed publications, patents, systems or products satisfy each and every limitation of the asserted claims of the '203 and '615 patents, either explicitly or inherently.

B. Obviousness

The following references constitute "obviousness references" herein:

- All references listed in (8) above;

[3] SRI has stipulated this is a 102(b) prior art reference.

[4] As discussed in Exhibit 6, section 1(A), Defendants request that the Court either (1) instruct the jury that Defendants need only prove invalidity by a preponderance of the evidence with respect to those issues on which PTO has initially rejected the claims during reexamination, or (2) instruct the jury that it may consider the PTO's decision to declare re-examinations and initially reject the claims-in-suit when determining whether or not Defendants have rebutted the presumption of validity and proven invalidity by clear and convincing evidence.

- All systems listed in (9) above;
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "A Method to Detect Intrusive Activity in a Networked Environment," Proc. 14th National Computer Security Conference, pp. 362-371, Oct. 1991;
- Emerald 1997 in combination with additional references regarding the Network Security Monitor, the Distributed Intrusion Detection System, the Graph Based Intrusion Detection System, the ISS RealSecure system, and the NetRanger system;
- SunScreen EFS Configuration and Management Guide, Release 1.1, Rev. A, Sun Microsystems, June 1997;
- CERT Advisory CA-1996-21 TCP Syn Flooding and IP Spoofing Attacks;
- CERT Advisory CA-1996-26 "Denial-of-Service Attack via Ping, Dec. 18, 1996.

11. Whether certain obviousness references are prior art under 35 U.S.C. § 102 (a), (b) or (e).

12. The level of ordinary skill in the art at the time of the invention of the '203 and '615 patents.

13. Whether, by clear and convincing evidence, Symantec can prove that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine certain obviousness references resulting in satisfaction of the limitations of the asserted claims of the '203 and '615 patents.

14. Whether, by clear and convincing evidence, Symantec can prove that it would have been obvious to one of ordinary skill in the art at the time of the invention to modify certain obviousness references resulting in satisfaction of the limitations of the asserted claims of the '203 and '615 patents.

15. Whether there is any objective evidence of nonobviousness for any asserted

patent claim, and whether SRI can prove a connection or nexus between any such objective evidence and the inventions of the asserted claims.

16. Whether there is any objective evidence of obviousness for any asserted patent claim.

C. Best Mode

17. Whether, by clear and convincing evidence, Symantec can prove that the common patent specification fails to disclose the best mode of practicing the asserted claims of the '203 and '615 patents.

D. Written Description

18. Whether, by clear and convincing evidence, Symantec can prove that the common patent specification fails to describe to one of ordinary skill in the art each and every claim of the '203 and '615 patents that requires "integrating" / "integrate" or "correlating."

III. UNENFORCEABILITY

19. Whether individuals associated with the filing or prosecution of the '203 and '615 patents either withheld information from the United States Patent & Trademark Office (the "PTO") or misrepresented information to the PTO, including the following as disclosed in Symantec's Response to SRI's Interrogatory No. 11:

- Debra Anderson, Thane Frivold, and Alfonso Valdes, "Next-Generation Intrusion Detection Expert Systems (NIDES): A Summary," SRI-CSL-95-07, May 1995;
- L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood, D. Wolber, "A Network Security Monitor," Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, May 1990;
- Y. Frank Jou et al., Architecture Design of a Scalable Intrusion Detection System for the Emerging Network, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997;
- Y. Frank Jou and S. Felix Wu, Scalable Intrusion Detection for the Emerging

Network Infrastructure, IDS Program Review, SRI July 1997;

- Additional prior art references disclosed in Symantec's Response to SRI's Interrogatory No. 11; and
- Inequitable conduct with regard to the filing of the Appendix to the '203 and '615 patents.

20. Whether, by clear and convincing evidence, Symantec can prove that the withheld or misrepresented information was material.

21. Whether, by clear and convincing evidence, Symantec can prove that the information was withheld or misrepresented with the intent to mislead or deceive the PTO.